

<<破译英格玛密码>>

图书基本信息

书名：<<破译英格玛密码>>

13位ISBN编号：9787533755881

10位ISBN编号：753375588X

出版时间：2013-7-1

出版时间：安徽科学技术出版社

作者：[波兰] 莱斯泽克·格拉乌斯基

译者：于素芳

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<破译英格玛密码>>

内容概要

莱斯泽克·格拉乌斯基编著的《破译英格玛密码——马里安·乔耶夫斯基的密码人生》写给那些想了解波兰数学家，印现代密码学之父马里安·雷耶夫斯基的生活与工作情况的人们。

《破译英格玛密码——马里安·乔耶夫斯基的密码人生》作者运用排列理论复制出了德国英格玛（Enigma）密码机，并找到了破译用该机加密信息的方法，这种方法早在二战爆发之前就已经影响到了二战未来的发展趋向。

关于破译英格玛密码对整个战争的影响，历史学家和军事理论家们仍然兴趣颇浓，争论不已。

<<破译英格玛密码>>

书籍目录

引言
序曲
第一幕 马里安·雷耶夫斯基登上历史舞台
第二幕 求学于哥廷根大学和波兹南大学
第三幕 就职于密码处
关于密码
单表替代密码——单字母密码
恺撒 (Caesar) 密码——一种转换密码
阿亨蒂 (Argenti) 密码——一种自动密钥式恺撒密码
密码分析学的诞生
多表替代密码 (Polyalphabetic substitution ciphers)
——渐进密钥式密码 (Progressive key ciphers)
特里特米乌斯密码 (The Trithemius)
维吉尼亚密码 (The Vigenere cipher)
卡斯基实验 (The Kasiski 's examination)
关于加密机
阿尔贝蒂 (Alberti) 圆盘
电汽加密机
电汽加密机的演变历程
军用英格玛加密机的秘密
军用英格玛加密机的内部构造
密钥 (Keys)
对军用英格玛加密机的攻击
会话密钥 (Session key) 的前置代码 (The prefix)
密钥传递
每日特征词 (Daily characteristics)
经验式方法 (The heuristic approach)
特征密钥法 (Characteristic keys)
统计方法
不同字母的密钥方法
AVA工厂
历史在前进
雷耶夫斯基个人生活的转机
字母循环表目录 (The catalogtle of cycles)
可能词 (Probable words) 的方法
巧合索引I (The index of coincidence)
加密机制的变化
战争时期
皮瑞会议
1939年9月大撤退
流亡法国
彷徨
尾声
附录A 后继有人
布莱奇利庄园

<<破译英格玛密码>>

巨人密码机

日本紫密机

附录B 换位密码 (Transposition ciphers)

格栅密码 (Rail fence cipher)

斯巴达天书 (The Spartan scytale , 公元前5世纪)

弗莱斯纳尔 (Fleissner) 模板

德国简单换位密码 (Single transposition cipher)

德国复式替换密码 (Double transposition cipher)

附录C 多表换位密码 (Polygraphic ciphers)

普莱费尔密码 (The Playfair cipher)

双打印盒密码 (The Doppelkastn-Vefahren)

<<破译英格玛密码>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>